

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 6 日
Date of Application:

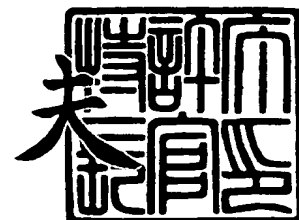
出 願 番 号 特 願 2 0 0 3 - 0 2 9 8 1 3
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 2 9 8 1 3]

出 願 人 インターナショナル・ビジネス・マシーンズ・コーポレーシ
Applicant(s): ョン

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 JP09030014
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/32
G06F 15/00

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内

【氏名】 緒方 栄次

【特許出願人】

【識別番号】 390009531

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【代理人】

【識別番号】 100108501

【弁理士】

【氏名又は名称】 上野 剛史

【復代理人】

【識別番号】 100085408

【弁理士】

【氏名又は名称】 山崎 隆

【手数料の表示】

【予納台帳番号】 117560

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706050

【包括委任状番号】 9704733

【包括委任状番号】 0207860

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラム

【特許請求の範囲】

【請求項 1】 セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア、

OS 起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が” 正” であれば OS 起動を許容する OS 起動許容手段、

所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段、

前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第 1 のシステム状態」と言う。）を生成する OS 起動であってかつ前記 OS 起動許容手段が作動する第 1 の形式の OS 起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第 2 のシステム状態」と言う。）を生成する OS 起動であってかつ前記 OS 起動許容手段が作動しない機能制限された第 2 の形式の OS 起動とのいずれかを選択して実施する OS 起動形式選択手段、

第 2 のシステム状態の期間に生成され第 1 の形式の OS 起動における前記 OS 起動許容手段の作動を無効にする無効化手段、及び

前記 OS 起動許容手段が前記無効化手段により作動を無効化された第 1 の形式の OS 起動が少なくとも 1 回、実施された後、前記無効化手段による前記 OS 起動許容手段の作動の無効を解除する無効解除手段、
を有していることを特徴とする情報処理装置。

【請求項 2】 ユーザ認証用の入力データは、第 1 の形式の OS 起動の際にユーザがキー入力するデータであることを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】 前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のもの

として生成されたものであり、補助記憶装置に保存されているものであることを特徴とする請求項 1 記載の情報処理装置。

【請求項 4】 第 1 及び第 2 の形式の OS 起動は、同一の補助記憶装置内に保存されている同一の OS に基づく起動であり、前記 OS 起動形式選択手段は、OS を起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第 1 の形式の OS 起動を、また、”有り”のときは第 2 の形式の OS 起動を、それぞれ選択して実施するものであることを特徴とする請求項 1 記載の情報処理装置。

【請求項 5】 第 1 及び第 2 の形式の OS 起動は、それぞれ別の補助記憶装置内に保存されている OS に基づく起動であり、前記 OS 起動形式選択手段は、前記第 2 の OS を保存する補助記憶装置から前記第 2 の OS を読み取り可能であるときは、第 1 の形式の OS 起動より第 2 の形式の OS 起動を優先して、選択し、実施するものであることを特徴とする請求項 1 記載の情報処理装置。

【請求項 6】 前記無効解除手段が前記無効化手段による前記 OS 起動許容手段の作動の無効を解除した後に、前記無効解除手段を消去する消去手段を有していることを特徴とする請求項 1 記載の情報処理装置。

【請求項 7】 前記消去手段は前記無効解除手段により生成されるものであることを特徴とする請求項 6 記載の情報処理装置。

【請求項 8】 セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア、

OS 起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であれば OS 起動を許容する OS 起動許容手段、

所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段、

前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第 1 のシステム状態」と言う。）を生成する OS 起動であってかつ前記 OS 起動許容手段が作動する第 1 の形式の OS 起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第 2 のシステ

ム状態」と言う。)を生成するOS起動であってかつ前記OS起動許容ステップが作動しない機能制限された第2の形式のOS起動とのいずれかを選択して実施するOS起動形式選択手段、

を有する情報処理装置の制御方法であって、

次の各ステップをコンピュータに実行させる情報処理装置の制御方法であって、

無効化手段が、それが生成された以降の第1の形式のOS起動における前記OS起動許容手段の作動を無効にする無効化ステップ、及び

前記OS起動許容手段が前記無効化手段により作動を無効化された第1の形式のOS起動が少なくとも1回、実施された後、無効解除手段が、前記無効化手段による前記OS起動許容手段の作動の無効を解除する無効解除ステップ、を有していることを特徴とする情報処理装置用制御方法。

【請求項9】 ユーザ認証用の入力データは、第1の形式のOS起動の際にユーザがキー入力するデータであることを特徴とする請求項8記載の情報処理装置用制御方法。

【請求項10】 前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであることを特徴とする請求項8記載の情報処理装置用制御方法。

【請求項11】 第1及び第2の形式のOS起動は、同一の補助記憶装置内に保存されている同一のOSに基づく起動であり、前記OS起動形式選択手段は、OSを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第1の形式のOS起動を、また、”有り”のときは第2の形式のOS起動を、それぞれ選択して実施するものであることを特徴とする請求項8記載の情報処理装置用制御方法。

【請求項12】 第1及び第2の形式のOS起動は、それぞれ別の補助記憶装置内に保存されているOSに基づく起動であり、前記OS起動形式選択手段は、前記第2のOSを保存する補助記憶装置から前記第2のOSを読み取り可能であるときは、第1の形式のOS起動より第2の形式のOS起動を優先して、選択

し、実施するものであることを特徴とする請求項 8 記載の情報処理装置用制御方法。

【請求項 13】 前記無効解除手段が前記無効化手段による前記 OS 起動許可手段の作動の無効を解除した後に、消去手段が前記無効解除手段を消去する消去ステップ、

を有していることを特徴とする請求項 8 記載の情報処理装置用制御方法。

【請求項 14】 前記無効解除手段が前記消去手段を生成するステップ、を有していることを特徴とする請求項 13 記載の情報処理装置用制御方法。

【請求項 15】 請求項 8～13 のいずれかの情報処理装置用制御方法における各ステップをコンピュータに実行させることを特徴とする情報処理装置用制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、パーソナル・コンピュータ等の情報処理装置、情報処理装置用制御方法及び情報処理装置用制御プログラムに係り、詳しくはセキュリティ・ハードウェアを装備しシステム・ログオン時にセキュリティ・ハードウェア内のセキュリティ・キー情報に基づいてユーザ認証を行うようになっている情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラムに関するものである。

【0002】

【従来の技術】

TCPA (Trusted Computing Platform Alliance: "http://www.trustedcomputing.org/tcpaasp4/index.asp") の規格に準拠したセキュリティ・チップを装備する PC (パーソナル・コンピュータ) では、セキュリティ・チップにおける所定の暗号プログラムやセキュリティ・キー情報を使用して、種々のセキュリティ処理、例えば、OS (Operating System: オペレーティング・システム) 起動を許可すべきか否かのユーザ認証、OS との連携によるファイルやフォルダの暗号化及び復号、デジタル証明書の保管、並びに各種アプリケーションにおけるユ

ーザ認証の統合化等を実施している。

【0003】

一方、特許文献1は、端末に接続された認証装置を介してICカード等のセキュリティ・ハードウェア内のセキュリティ・キー情報を読み取り、セキュリティ・キー情報に基づきセキュリティ・ハードウェアの所有者が正当な所有者であるか否かを判断し、判断結果が正であるときのみ、端末からホストへのログインを許容している。

【0004】

【特許文献1】

特開2001-99466号

【0005】

【発明が解決しようとする課題】

PCにおいて通常のハードウェアの故障に係る修理では、故障したハードウェアを新規なものと交換すれば足りる。これに対して、TCPA準拠のセキュリティ・チップの交換を含む修理を行う場合には、交換後の新規なセキュリティ・チップには、交換前のセキュリティ・チップ内に保存していたセキュリティ・キー情報が存在しないので、セキュリティ・チップの交換後にPCに電源投入しても、OS起動（以下、適宜、「システム・ログオン」と言う。）ができず、すなわち、PCの使用が困難になる。すなわち、セキュリティ・チップ内のセキュリティ・キー情報は、セキュリティ・チップ内の所定のプログラムにより暗号化されて、セキュリティ・チップ内に保存されており、セキュリティ・キー情報に基づくシステム・ログオン用ユーザ認証を行うためには、セキュリティ・チップ内のセキュリティ・キー情報をセキュリティ・チップ内のプログラムにより復号する必要がある、セキュリティ・チップ内にセキュリティ・キー情報が無いと、この復号は困難になるので、ユーザ認証が実施できず、システム・ログオンが困難になる。これを克服するには、PCへOSを再インストールしてから、セキュリティ・キー情報を新規に設定し直す必要がある、労力と時間が膨大になる。また、交換前のセキュリティ・チップ内のセキュリティ・キー情報に基づいて暗号化されてハード・ディスクに保存されているフォルダやファイルは、交換前のセキュ

リティ・チップのセキュリティ・キー情報に基づいて暗号化されているので、新規のセキュリティ・チップについて別途、新規のセキュリティ・キー情報を登録しても、復号は困難である。TCPA準拠のセキュリティ・チップは、通常、マザーボードに組み付けられており、典型的な修理では、マザーボードのどれかの素子が故障したときには、マザーボード全体が交換されるので、セキュリティ・チップ自体は壊れていなくても、セキュリティ・チップが交換されるケースは多い。

【0006】

特許文献1は、正当なセキュリティ・ハードウェアに基づいて認証を受けて、一度、端末からホストへログインした後、セキュリティ・ハードウェアが悪意に正当なものから不正なものへ交換されて、セッションが継続する事態に対処するための方策は開示しているものの、正当なユーザが、セキュリティ・ハードウェアを交換したときに、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を使用しなければ、システム・ログオンして、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を新規なセキュリティ・ハードウェアに復元できない場合に、セキュリティ・キー情報を交換後のセキュリティ・ハードウェアに復元する有効な方策についてはなんら開示していない。

【0007】

本発明の目的は、システム・ログオンするためには交換前のセキュリティ・ハードウェアのセキュリティ・キー情報が必要であり、また、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を交換後のセキュリティ・ハードウェアに復元するためには、システム・ログオンする必要がある情報処理装置において、交換後の新規のセキュリティ・ハードウェアに交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を復元できる情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラムを提供することである。

【0008】

【課題を解決するための手段】

本発明の情報処理装置は次のものを有している。

・セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア

- ・ OS 起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が” 正 ” であれば OS 起動を許容する OS 起動許容手段
- ・ 所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段
- ・ 前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第 1 のシステム状態」と言う。）を生成する OS 起動であってかつ前記 OS 起動許容手段が作動する第 1 の形式の OS 起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第 2 のシステム状態」と言う。）を生成する OS 起動であってかつ前記 OS 起動許容手段が作動しない機能制限された第 2 の形式の OS 起動とのいずれかを選択して実施する OS 起動形式選択手段
- ・ 第 2 のシステム状態の期間に生成され第 1 の形式の OS 起動における前記 OS 起動許容手段の作動を無効にする無効化手段
- ・ 前記 OS 起動許容手段が前記無効化手段により作動を無効化された第 1 の形式の OS 起動が少なくとも 1 回、実施された後、前記無効化手段による前記 OS 起動許容手段の作動の無効を解除する無効解除手段

【0009】

本発明によれば、第 1 の形式の OS 起動とは別の形式としての第 2 の形式の OS 起動を利用する。第 1 の形式の OS 起動とは、例えば、標準の OS 起動であり、機能制限の無いシステム状態に情報処理装置を立ち上げるときの OS 起動である。これに対して、第 2 の形式の OS 起動とは、例えば、非常時又は緊急避難時の OS 起動であり、最小限の機能で情報処理装置を作動させるシステム状態を確保するときの OS 起動である。例えば OS として Windows NT, Windows 2000, Windows XP（いずれも登録商標）を装備する PC（パーソナル・コンピュータ）では、標準の OS 起動は、ユーザが PC の電源投入するのみで、他の特別のユーザ操作を要求されずに、実行されるものである。これに対して、第 2 の形式の OS 起動としてのセーフ・モード用 OS 起動は、ユーザが、PC の電源投入後、例えばキー・ボードの F8 キーを押し続けるとい

う所定のユーザ操作があったときに実行される。第2の形式のOS起動では、機能制限のために、セキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証をスキップして、情報処理装置を第2のシステム状態にすることができる。第2のシステム状態期間では、機能制限のために、セキュリティ・ハードウェアのセキュリティ・キー情報の復元処理は困難であるが、以降の第1の形式のOS起動におけるセキュリティ・ハードウェアのセキュリティ・キー情報に係る認証処理の無効化等の設定は可能である。なぜなら、これらの設定は、低レベルの機能であり、第2のシステム状態では、所定レベル以下の機能の実行は可能であるからである。第2のシステム状態の例としてのセーフ・モードでは、FD（フロッピー・ディスク）からハード・ディスクへのプログラム・ファイルのコピーや、次回以降の標準モードの起動における設定は可能である。こうして、第2のシステム状態における所定のプログラムの実行により、無効化手段を含むコンピュータ・ソフトウェアが生成される。無効化手段は、それが生成された以降の第1の形式のOS起動の際には、OS起動許容手段の作動を無効化し、これにより、OS起動許容手段によるユーザ認証を経ずに、情報処理装置を第1のシステム状態にすることができる。こうして実現された第1のシステム状態において、セキュリティ・ハードウェアにおけるセキュリティ・キー情報が復元される。無効解除手段は、次回からの第1の形式のOS起動では、OS起動許容手段によるセキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証処理を有効化するように、作動する。結果、新規のセキュリティ・ハードウェアに交換された情報処理装置において、交換前のセキュリティ・ハードウェアを装備していた情報処理装置のときと同一のセキュリティ・キー情報に基づくシステム・ログオン及びその他の処理が実施される。

【0010】

本発明の情報処理装置は、上述の情報処理装置に対して、次の(a1)～(a6)の1個又は複数個を任意の組み合わせで付加したものを含む。

(a1) ユーザ認証用の入力データは、第1の形式のOS起動の際にユーザがキー入力するデータであること。

(a2) 前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・

キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであること。

(a 3) 第1及び第2の形式のOS起動は、同一の補助記憶装置内に保存されている同一のOSに基づく起動であり、前記OS起動形式選択手段は、OSを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第1の形式のOS起動を、また、”有り”のときは第2の形式のOS起動を、それぞれ選択して実施するものであること。

(a 4) 第1及び第2の形式のOS起動は、それぞれ別の補助記憶装置内に保存されているOSに基づく起動であり、前記OS起動形式選択手段は、前記第2のOSを保存する補助記憶装置から前記第2のOSを読み取り可能であるときは、第1の形式のOS起動より第2の形式のOS起動を優先して、選択し、実施するものであること。

(a 5) 前記無効解除手段が前記無効化手段による前記OS起動許容手段の作動の無効を解除した後に、前記無効解除手段を消去する消去手段をさらに有していること。

(a 6) 上記(a 5)において、前記消去手段は前記無効解除手段により生成されるものであること。

【0011】

本発明の情報処理装置用制御方法が適用される情報処理装置は、セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェアと、OS起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればOS起動を許容するOS起動許容手段と、所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段と、前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第1のシステム状態」と言う。）を生成するOS起動であってかつ前記OS起動許容手段が作動する第1の形式のOS起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第2のシステム状態」と言う。）を生成するOS起動で

あつてかつ前記OS起動許容ステップが作動しない機能制限された第2の形式のOS起動とのいずれかを選択して実施するOS起動形式選択手段と、を有する。
そして、本発明の情報処理装置用制御方法は次のステップを有している。

- ・無効化手段が、それが生成された以降の第1の形式のOS起動における前記OS起動許容手段の作動を無効にするように、第2のシステム状態の期間に前記無効化手段を生成する無効化手段生成ステップ

- ・前記OS起動許容手段が前記無効化手段により作動を無効化された第1の形式のOS起動が少なくとも1回、実施された後、無効解除手段が、前記無効化手段による前記OS起動許容手段の作動の無効を解除するように、前記無効解除手段を生成する無効解除手段生成ステップ

【0012】

本発明の情報処理装置用制御方法は、上述の情報処理装置用制御方法に対して、次の(b1)～(b6)の1個を又は複数個を任意の組み合わせで付加したものを含む。

【0013】

(b1) ユーザ認証用の入力データは、第1の形式のOS起動の際にユーザがキー入力するデータであること。

(b2) 前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであること。

(b3) 第1及び第2の形式のOS起動は、同一の補助記憶装置内に保存されている同一のOSに基づく起動であり、前記OS起動形式選択手段は、OSを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第1の形式のOS起動を、また、”有り”のときは第2の形式のOS起動を、それぞれ選択して実施するものであること。

(b4) 第1及び第2の形式のOS起動は、それぞれ別の補助記憶装置内に保存されているOSに基づく起動であり、前記OS起動形式選択手段は、前記第2のOSを保存する補助記憶装置から前記第2のOSを読み取り可能であるときは、第1の形式のOS起動より第2の形式のOS起動を優先して、選択し、実施する

ものであること。

(b 5) 前記無効解除手段が前記無効化手段による前記OS起動許容手段の作動の無効を解除した後に、消去手段が前記無効解除手段を消去する消去ステップを有していること。

を有していることを特徴とする請求項8記載の情報処理装置。

(b 6) 上記(b 5)のステップに加えて、前記無効解除手段が前記消去手段を生成するステップを有していること。

【0014】

本発明の情報処理装置用制御プログラムは、本発明の情報処理装置用制御方法における各ステップをコンピュータに実行させる。

【0015】

【発明の実施の形態】

以降、本発明を実施の形態について具体的に説明する。なお、本発明は実施の形態及び実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。図面全般にわたる構成を先に説明してから、情報処理装置10の修理者によるセキュリティ・キー情報の復元作業の手順に則して、情報処理装置10の作用について説明する。

【0016】

図1は情報処理装置10のブロック図である。図1において、無効化手段15のブロックは斜線を施されているが、これは、無効化手段15が第2のシステム状態において生成されることを意味する。なお、無効解除手段16は、無効化手段15によるOS起動許容手段12の作動無効後に、該無効を解除するように設定してあれば、第1のシステム状態ではなく、無効化手段15と同様に、第2のシステム状態において生成されてもよい。無効解除手段16は、例えば、無効化手段15がOS起動許容手段12の作動を無効にした第1の形式のOS起動による第1のシステム状態において生成される。セキュリティ・ハードウェア11は、セキュリティ・キー情報を読書き自在に格納(ストア)する。OS起動許容手段12は、OS起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア11から読み出したセキュリティ・キー情報に基づい

て判断し、該判断結果が” 正” であればOS起動を許容する。セキュリティ・キー情報復元手段13は、所定の復元用データに基づいてセキュリティ・ハードウェア11にセキュリティ・キー情報を復元する。OS起動形式選択手段14は、セキュリティ・キー情報復元手段13が作動可能となるシステム状態（以下、「第1のシステム状態」と言う。）を生成するOS起動であってかつOS起動許容手段12が作動する第1の形式のOS起動と、セキュリティ・キー情報復元手段13が作動不可能である機能制限されたシステム状態（以下、「第2のシステム状態」と言う。）を生成するOS起動であってかつOS起動許容手段12が作動しない機能制限された第2の形式のOS起動とのいずれかを選択して実施する。無効化手段15は、第2のシステム状態の期間に生成され、第1の形式のOS起動におけるOS起動許容手段12の作動を無効にする。注釈すると、無効化手段15は、第1の形式のOS起動におけるOS起動許容手段12の作動を無効にする処理を実施するが、該処理は、当然に、それが生成されてからのことであり、生成前に該処理の実施は困難である。OS起動許容手段12が無効化手段15により作動を無効化された第1の形式のOS起動が少なくとも1回、実施された後、無効化手段15によるOS起動許容手段12の作動の無効を解除する。

【0017】

典型的には、OS起動許容手段12が無効化手段15により作動を無効化された第1の形式のOS起動が1回だけ、実施されしだい、無効化手段15によるOS起動許容手段12の作動の無効を解除する。しかし、無効解除の時期は、第1の形式のOS起動が複数の所定回数、実施された後であったり、1回目の実施時刻から所定時間経過後の最初の第1の形式のOS起動の時又は第1のシステム状態の期間であってもよい。

【0018】

図2は携帯型PC（パーソナル・コンピュータ）18及びデスク・トップ型PC19を示す。情報処理装置10は、例えば、携帯型PC38及びデスク・トップ型PC39であり、さらに、その他のPC、PDA（Personal Digital Assistant）、携帯電話、家電、及びゲーム機であってもよい。

【0019】

セキュリティ・ハードウェアは、マザーボード上のセキュリティ・チップに制限されず、ICカードや、さらに、PCのUSB (Universal Serial Bus) 等の周辺機器接続用コネクタに、ケーブルを介さずに直接、差し込まれる携帯型メモリ・デバイス等の他のセキュリティ・ハードウェアであってもよい。セキュリティ・チップは典型的にはEEPROM (Electrically Erasable Programmable Read-Only Memory。電氣的に消去(書き換え)できるROM) である。OSは、情報処理装置がPCである場合は、例えば、Windows NT, Windows 2000, Windows XP、DOS (いずれも登録商標) のほか、Linux、Mac OS (登録商標)、及びTRON用OS等、他のOSであってもよい。OSがWindowsである場合、第1及び第2のシステム状態はそれぞれ標準モード及びセーフ・モードに対応する。

【0020】

ユーザ認証用の入力データは、例えば第1の形式のOS起動の際にユーザがキー入力するデータである。図3はセキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証用の窓を例示したものである。図3の窓は、情報処理装置10としてのPCでは、第1の形式のOS起動の際にPCのディスプレイに表示される。ユーザは、図3の窓に対して、ユーザ名の欄及びパスフレーズの欄に、自己に係るユーザ名及びパスフレーズ(例: "本日は晴天なり") を、キーボードを使って入力する。その次に、"OK" ボタンをクリックすると、ユーザ名及びパスフレーズがCPUに取り込まれ、セキュリティ・ハードウェア11内のセキュリティ・キー情報に係るデータと照合され、ユーザが正当であると認証されれば、第1の形式のOS起動が実行される。OS起動の際にユーザ認証用の入力データは、ユーザがキーボードを介して入力するパスワードやパスフレーズに限定されず、ユーザから検出したユーザの指紋や虹彩に係るデータであってもよい。

【0021】

図4はOSに基づくユーザ認証用窓の例示である。システム・ログオン時におけるOSに基づくユーザ認証は、図3に係るセキュリティ・ハードウェア11のセキュリティ・キー情報に基づくユーザ認証は、図4に係るシステム・ログオン

時におけるOSに基づくユーザ認証とは別個のものである。ユーザは、図4のユーザ認証用窓に対してユーザ名及びパスワードを各欄に入力する。PCのセキュリティのためにセキュリティ・ハードウェア11としてのセキュリティ・チップをPCにおいて利用するソフトウェア（以下、該ソフトウェアを「CSS（Client Security Software）」と呼ぶことにする。）は、セキュリティ・チップを装備したPCを購入したユーザがインターネットの所定のサイトより適宜、PCへダウンロードするようになっており、該CSSでは、OSや各アプリケーションでの認証を、システム・ログオン時のセキュリティ・チップのセキュリティ・キー情報に基づく認証に統合できるようになっている。すなわち、CSSでは、設定により、PCのユーザは、システム・ログオン時に、セキュリティ・チップのセキュリティ・キー情報に基づく認証を1回、受けさえすれば、そのシステム・ログオン中、繰返して他のユーザ認証を受けなくて済むようになっている。

【0022】

復元用データは、例えば、セキュリティ・ハードウェア11内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、ハード・ディスクのような補助記憶装置に保存されているものである。図5はセキュリティ・ハードウェア11におけるセキュリティ・キー情報を復元する際の作業窓を例示する。CSSは、システム・ログオンの許可等のユーザ認証、OSとの連携によるファイルやフォルダの暗号化及び復号、デジタル証明書の保管、並びに各種アプリケーションにおけるユーザ認証の統合化の他に、セキュリティ・チップへのセキュリティ・キー情報の新規登録、セキュリティ・チップへ登録済みのセキュリティ・キー情報の削除、及びセキュリティ・キー情報の復元の機能を装備している。CSSでは、セキュリティ・キー情報を作成する際、セキュリティ・キー情報の復元を実現するための復元実現用ファイルが該セキュリティ・キー情報の対として生成される。このような復元実現用ファイルは、好ましくは、FDにアーカイブ・ファイルによりストアしておき、情報処理装置10のユーザは、該FDを適切な場所に保管しておく。しかし、復元実現用アーカイブ・ファイルはハード・ディスクに保存してもよい。復元実現

用アーカイブ・ファイルを所定のFDに保管しておくときは、情報処理装置10の修理者は、ユーザより該FDを預かるか、ユーザよりメールで送付して貰うか、予めハード・ディスクの所定のフォルダにストアしておいて貰うか等する。修理者は、図5のセキュリティ・キー情報復元用窓において、復元実現用アーカイブ・ファイル、公開鍵ファイル、及び秘密鍵ファイルをそれぞれの入力欄にパスと共に入力する。この入力は、ユーザが直接書き込むことに代えて、“参照”ボタンをクリックして、所定のドライブの所定のフォルダにアクセスして、該当のファイルを選択することにより、実施可能となっている。3個の入力欄に該当のファイルの入力が終わったら、修理者は、“OK”ボタンをクリックする。こうして、3個の入力欄に入力されたファイルの対応が取れていることが復元実現用アーカイブ・ファイルにより検証されると、セキュリティ・チップには、セキュリティ・キー情報が復元される。なお、CSSでは、復元実現用ファイルとしてのアーカイブ・ファイル、公開鍵及び秘密鍵の3個の要素からパスフレーズを知ることは可能であるが、アーカイブ・ファイルのみからパスフレーズを知ることが困難になっている。したがって、アーカイブ・ファイルをストアしたFDを盗み出されても、盗用者がパスフレーズを知ることはできない。

【0023】

図6は所定態様のOS起動形式選択手段14を装備する情報処理装置10のブロック図である。第1及び第2の形式のOS起動は、同一の補助記憶装置21（典型的にはハード・ディスク）内に保存されている同一のOS22に基づく起動である。図6のOS起動形式選択手段14は、第1及び第2の形式のOS起動の実施手段23、24、所定ユーザ操作の検出手段25、及び切替手段26、を有している。所定ユーザ操作の検出手段25は、OS22を起動しようとするときに、所定ユーザ操作の有無を検出する。切替手段26は、該所定ユーザ操作が“無し”であるときは第1の形式のOS起動の実施手段23を作動させ、また、“有り”であるときは第2の形式のOS起動の実施手段24を作動させる。

【0024】

図7は別の所定態様のOS起動形式選択手段14を装備する情報処理装置10のブロック図である。第1及び第2の形式のOS起動は、それぞれ別の補助記憶

装置 21, 31 内に保存されている OS 22, 32 に基づく起動である。補助記憶装置 21, 31 は例えばそれぞれハード・ディスク及び FD (フロッピー・ディスク) である。典型的には、補助記憶装置 21 は常設補助記憶装置であり、補助記憶装置 31 は交換可能なメディアである。図 7 の OS 起動形式選択手段 14 は、第 1 及び第 2 の形式の OS 起動の実施手段 23, 24、メディア検出手段 34、及び切替手段 26、を有している。メディア検出手段 34 は、OS 32 が保存されている補助記憶装置 31 から OS 32 を読み取り可能であるか否かを検出する。情報処理装置 10 は、OS をもつ交換可能メディアがそのメディア用ドライブに存在すれば、OS をもつ常備メディアより優先して、交換可能メディアから OS を読み取る方式を採用するので、切替手段 26 は、第 2 の形式の OS 起動 32 を保存する補助記憶装置 31 から第 2 の OS 32 を読み取り可能であるときは、第 2 の形式の OS 起動の実施手段 24 を作動させ、また、不可能であるときは、第 1 の形式の OS 起動の実施手段 23 を作動させる。

【0025】

図 8 は消去手段 37 が付加された情報処理装置 10 のブロック図である。消去手段 37 は、無効解除手段 16 が無効化手段 15 による OS 起動許容手段 12 の作動の無効を解除した後に、無効解除手段 16 を消去する。消去手段 37 は例えば前記無効解除手段 16 により生成されるものである。無効化手段 15 及び無効解除手段 16 はソフトウェアの機能として実現されるが、該ソフトウェアを所有するものは修理者等の特定の者に限定されることが管理上、望ましい。この場合、修理者は、作業実行後は情報処理装置 10 から分離できる FD 等の交換可能なメディアから該ソフトウェアを立ち上げ、情報処理装置 10 に常備のハード・ディスクには、作業終了後に該ソフトウェアの主要部としての無効化手段 15 及び無効解除手段 16 が残らないようにする必要がある。無効化手段の 15 の機能、すなわち次回以降の第 1 の形式の OS 起動において OS 起動許容手段 12 の作動を無効にする設定は、第 2 のシステム状態において交換可能メディアから実行して、ハード・ディスク内に該ソフトをストアすることを回避できるが、無効解除手段 16 を構成するソフトウェア部分は、第 2 のシステム状態では実行できず、ハード・ディスクにコピーして、実行する必要が生じることがある。しかし、無

無効解除手段 16 がその機能を実行した直後の期間、例えば次の第 1 のシステム状態の期間において、プログラム・ファイル削除プログラムのような消去手段 37 が無効解除手段 16 を消去するようにすれば、無効解除手段 16 を構成するソフトウェア部分はハード・ディスクに残ったまま、修理者からユーザに情報処理装置 10 が返却されることが防止される。

【0026】

修理者が情報処理装置 10 におけるセキュリティ・ハードウェア 11 を交換した修理作業を行ったときに、修理者がセキュリティ・ハードウェア 11 にセキュリティ・キー情報を復元する処理手順 (R1) ~ (R6) を説明しつつ、情報処理装置 10 の作用を説明する。OS が Windows である場合、第 1 及び第 2 の形式の OS 起動はそれぞれ例えば標準モード及びセーフ・モードの OS 起動に対応する。標準モードの OS 起動は、ユーザ (修理者も含む。) が、PC の電源スイッチを”入”にするのみで、実施される。これに対して、セーフ・モードの OS 起動は、PC の電源スイッチを”入”にすることの他に、ファンクション・スイッチ F8 を押す等、他の操作を要求される。したがって、所定のユーザ操作が行われたか否かを検知することにより、標準モード及びセーフ・モードのどちらの OS 起動を行うべきかを判断できる。セーフ・モードのシステム状態は、標準モードのシステム状態に対して、機能が制限されている。セーフ・モードの OS 起動及びシステム状態では、所定のトラブルにもかかわらず、PC の作動を確保するために、必要最小限の機能のみが可能になっている。したがって、OS 起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア 11 から読み出したセキュリティ・キー情報に基づいて判断する処理 (以下、「セキュリティ・キー情報に基づくユーザ認証処理」と言う。) は第 2 の形式の OS 起動ではスキップされ、すなわち実施されず、また、第 2 の形式の OS 起動に基づくシステム状態としての第 2 のシステム状態では、高機能型のアプリケーションは実行不能になるか、低機能のみの通常のアプリケーションの実行は困難になっている。なお、セーフ・モードのシステム状態において、FD (フロッピー・ディスク) 内のファイルをハード・ディスクへコピーする等の処理は可能であり、所定レベル以下の機能しかもたないプログラムの実行も可能である。

【0027】

(R1) 情報処理装置10において第2のシステム状態を実施し、情報処理装置10を第2の形式のOS起動にする。図6のOS起動形式選択手段14では、第1及び第2の形式のOSの起動のどちらを実行するかを、所定ユーザ操作の検出手段25による所定ユーザ操作の有無の検出に基づいて判断する。例えば、OSがWindowsである場合、OS起動形式選択手段14は、情報処理装置10の電源スイッチが”入”にされた後、キーボードのF8キーを押し続けると言うユーザ操作があれば、第2の形式のOS起動としてのセーフ・モード起動を実行し、該ユーザ操作がなければ、第1の形式のOS起動としての標準モード起動を実行する。図7のOS起動形式選択手段14では、第1及び第2のシステム状態のいずれを実行するかを、OS32をストアしている補助記憶装置31がそれ用のドライブ（該ドライブは、システムへ接続状態になっていれば、内付け及び外付けのどちらでも可）に存在するか否かに基づいて判断する。一般のPCでは、FDドライブやCDドライブにOSを読み取り自在のFDやCD-ROM等のメディアがあった場合、ハード・ディスクのOSより優先して交換可能メディアからOSを読み取って、それを起動するようになっている。セーフ・モードのためのOS起動や補助記憶装置31のOS32の起動では、機能が十分に制限された必要最小限機能の起動となるので、OS起動時のセキュリティ・キー情報に基づくユーザ認証は省略され、図3の窓は表示されることなく、OS起動が進み、情報処理装置10は第2のシステム状態となる。

【0028】

(R2) 修理者は、情報処理装置が第2の形式のOS起動になった後、所定のプログラム（該プログラムの名前を説明の便宜上、”CSSRT (Client Security Software Repair Tool)”と呼ぶことにする。）がストアされているFDをFD用のドライブにセットし、プログラムCSSRTを実行する。なお、FD用ドライブは、PCに内蔵されていてもよいし、USB (Universal Serial Bus) ケーブルを介してPC本体に分離自在に接続されるものであってもよい。プログラムCSSRTは、無効化手段15の機能を果たすCSSRT本体と無効解除手段16の機能を果たす部分CSSRT__1

とを含み、部分CSSRT__1を、FDから補助記憶装置としてのハード・ディスクにコピーするか、自ら作成してハード・ディスクにストアする。

【0029】

(R3) プログラムCSSRTの終了に伴い、情報処理装置10は自動的に又は修理者の指示によりリスタート(Restart)する。注意すべきは、このリスタート時において、プログラムCSSRT__1は、ハード・ディスクに残っているが、CSSRT本体は情報処理装置10のどこにも残らないことである。

【0030】

(R4) 修理者は、起動時に、所定ユーザ操作、例えばキーボードのF8キーを押し続けるというような所定ユーザ操作を省略する。OS起動形式選択手段14は、所定のユーザ操作の有無を検出し、切替手段26は、第1の形式のOS起動の実施手段23を作動させて、第1の形式のOS起動を実行する。OS起動許容手段12は、今回の第1の形式のOS起動においては、無効化手段15により作動を無効化されているので、修理者に対してOS起動の許容のための図3のパスフレーズ、すなわちセキュリティ・チップのセキュリティ・キー情報に基づく認証としての認証用データの入力を求めない。こうして、情報処理装置10は第1のシステム状態となる。なお、無効解除手段16の機能を果たすCSSRT__1は、無効解除手段16の機能を果たすとともに、その機能終了後に自分自身としてのCSSRT__1を削除する削除プログラムCSSRT__1__DEL(図8の消去手段37に相当するプログラム)を、CSSRT__1の存命中に作る。こうして、ハード・ディスク等の常備補助記憶装置に無効化処断15及び無効解除手段16が存在する期間は、極めて限定されたものとなる。なお、典型的には、CSSRT__1は、無効解除手段16の機能実施後に、CSSを呼び出す機能も実施する。

【0031】

(R5) 修理者は、(R4)の後の第1のシステム状態において、セキュリティ・ハードウェア11へのセキュリティ・キー情報の復元作業を行う。セキュリティ・キー情報復元手段13は、所定の復元用データに基づいて復元したセキュリティ・キー情報をセキュリティ・ハードウェア11へ書き込む。CSSでは、図

5を参照して前述したように、ハード・ディスク内の復元用データ・ファイルに基づいてセキュリティ・キー情報の復元が可能になっている。セキュリティ・キー情報復元手段13は、例えば、図5のセキュリティ・キー情報復元用窓を介して入力された復元用データに基づいてセキュリティ・ハードウェア11にセキュリティ・キー情報を復元する。

【0032】

(R6) セキュリティ・キー情報復元手段13によるセキュリティ・ハードウェア11におけるセキュリティ・キー情報を復元したのに伴い、情報処理装置10は、自動的に又は修理者の所定の指示を待ってリスタートする。CSSRT__1__DELは、このリスタート時に、又はCSSRT__1の実行終了後でかつリスタート前の第1のシステム状態の期間に、作動して、CSSRT__1を削除するので、このリスタートでは、第1の形式のOS起動にもかかわらず、無効化手段15は作動せず、セキュリティ・キー情報に基づくユーザ認証が実施される。

【0033】

消去手段37の機能を実現するプログラムはハード・ディスクに残っていても、特に弊害はない。また、万一、無効解除手段16に係るプログラムが常備補助記憶装置に残ったまま、修理者からユーザに情報処理装置10が返却されたとしても、ユーザが自分のユーザ認証を要求されるということであり、不利なことは、使用しない余計なプログラムがハード・ディスクに残っているということだけである。

【0034】

図9は図10のフローチャートに係るプログラムを実行するためのハードウェア構成図である。図10のフローチャートに係る方法の各ステップは例えば図9のハードウェアを使用して実行される。システム・バス43には、CPU44、主記憶装置45及び入出力装置46が接続される。後述の図10のフローチャートに係る方法は、コード化されたプログラムとして実行可能となっている。入出力装置46には、該プログラムをストアしてあるハード・ディスク等の補助記憶装置が含まれ、該プログラムは、CPU44において実行されるのに先立ち、主記憶装置45にストアされる。CPU44は、主記憶装置45の命令行を順次、

読み出して、該プログラムを実行する。

【0035】

図10は情報処理装置10の制御方法のフローチャートである。該制御方法が適用される情報処理装置10は、図1に記載されている通り、セキュリティ・ハードウェア11、OS起動許容手段12、セキュリティ・キー情報復元手段13、及びOS起動形式選択手段14を有している。セキュリティ・ハードウェア11は、セキュリティ・キー情報を読書き自在に格納する。OS起動許容手段12は、OS起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア11から読み出したセキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればOS起動を許容する。セキュリティ・キー情報復元手段13は、所定の復元用データに基づいてセキュリティ・ハードウェア11にセキュリティ・キー情報を復元する。OS起動形式選択手段14は、セキュリティ・キー情報復元手段13が作動可能となるシステム状態（以下、「第1のシステム状態」と言う。）を生成するOS起動であってかつOS起動許容手段12が作動する第1の形式のOS起動と、セキュリティ・キー情報復元手段13が作動不可能である機能制限されたシステム状態（以下、「第2のシステム状態」と言う。）を生成するOS起動であってかつOS起動許容ステップが作動しない機能制限された第2の形式のOS起動とのいずれかを選択して実施する。図10のフローチャートにおいて、S50では、無効化手段15が、それが生成された以降の第1の形式のOS起動におけるOS起動許容手段12の作動を無効にする。S51では、OS起動許容手段12が無効化手段により作動を無効化された第1の形式のOS起動が少なくとも1回、実施された後、無効解除手段16が、無効化手段15による前記OS起動許容手段12の作動の無効を解除する。

【0036】

こうして、セキュリティ・ハードウェア11を交換したときのセキュリティ・キー情報の復元では、修理者は、セキュリティ・ハードウェア11のセキュリティ・キー情報に基づくOS起動許容手段12によるユーザ認証をスキップできる第2の形式のOS起動により情報処理装置10を第2のシステム状態にする。この後、プログラムの実行により、無効化手段15が生成され、該無効化手段15

は、次の第1の形式のOS起動において、セキュリティ・ハードウェア11のセキュリティ・キー情報に基づくOS起動許容手段12による認証を無効化させ、情報処理装置10を、セキュリティ・ハードウェア11におけるセキュリティ・キー情報の無存在にもかかわらず、第1のシステム状態にする。この第1のシステム状態の期間では、セキュリティ・ハードウェア11におけるセキュリティ・キー情報の復元可能であり、セキュリティ・キー情報復元手段13はセキュリティ・キー情報を復元する。無効解除手段16は、無効化手段15によるOS起動許容手段12の作動の無効を解除し、これにより、次の第1の形式のOS起動からは再び、セキュリティ・ハードウェア11のセキュリティ・キー情報に基づくOS起動許容手段12によるユーザ認証が実施される。

【0037】

図10のフローチャートに係る制御方法を適用される情報処理装置10には、次の態様(c1)～(c6)の1個又は複数個を任意の組み合わせで付加したものを含む。

(c1) ユーザ認証用の入力データは、第1の形式のOS起動の際にユーザがキー入力するデータである。

(c2) 復元用データは、セキュリティ・ハードウェア11内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置21に保存されているものである。

(c3) 第1及び第2の形式のOS起動は、同一の補助記憶装置21内に保存されている同一のOS22に基づく起動であり、OS起動形式選択手段14は、OS22を起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第1の形式のOS起動を、また、”有り”のときは第2の形式のOS起動を、それぞれ選択して実施するものである。

【0038】

(c4) 第1及び第2の形式のOS起動は、それぞれ別の補助記憶装置21, 31内に保存されているOSに基づく起動であり、OS起動形式選択手段14は、第2のOS32を保存する補助記憶装置31から第2のOS32を読み取り可能であるときは、第1の形式のOS起動より第2の形式のOS起動を優先して、選

択し、実施するものである。

(c5) 無効解除手段16が無効化手段15によるOS起動許容手段12の作動の無効を解除した後に、消去手段37が無効解除手段16を消去する消去ステップを有していること。

(c6) 上記(c5)のステップに加えて、無効解除手段16が消去手段37を生成するステップを有していること。

【0039】

図11は図10のフローチャートに上記(c5)及び(c6)に対応するステップを付加したフローチャートである。S53は、S51とS54との間に配置されてもよい。S53では、無効解除手段16が消滅手段37を生成する。S54では、消滅手段37が無効解除手段16を消去する。

【0040】

【発明の効果】

本発明によれば、OS起動時にセキュリティ・ハードウェアのセキュリティ・キー情報に基づいてユーザ認証を行う情報処理装置において、故障修理等のためにセキュリティ・ハードウェアを交換したときに、新規なセキュリティ・ハードウェアに旧セキュリティ・ハードウェアのセキュリティ・キー情報を復元することができる。

【図面の簡単な説明】

【図1】

情報処理装置のブロック図である。

【図2】

携帯型PC及びデスク・トップ型PCを示す図である。

【図3】

セキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証用の窓を例示した図である。

【図4】

OSに基づくユーザ認証用窓の例示した図である。

【図5】

セキュリティ・ハードウェアにおけるセキュリティ・キー情報を復元する際の作業窓を例示した図である。

【図 6】

所定態様の OS 起動形式選択手段を装備する情報処理装置のブロック図である。

【図 7】

別の所定態様の OS 起動形式選択手段を装備する情報処理装置のブロック図である。

【図 8】

消去手段が付加された情報処理装置のブロック図である。

【図 9】

図 10 のフローチャートに係るプログラムを実行するためのハードウェア構成図である。

【図 10】

情報処理装置の制御方法のフローチャートである。

【図 11】

図 10 にさらに所定のステップを付加したフローチャートである。

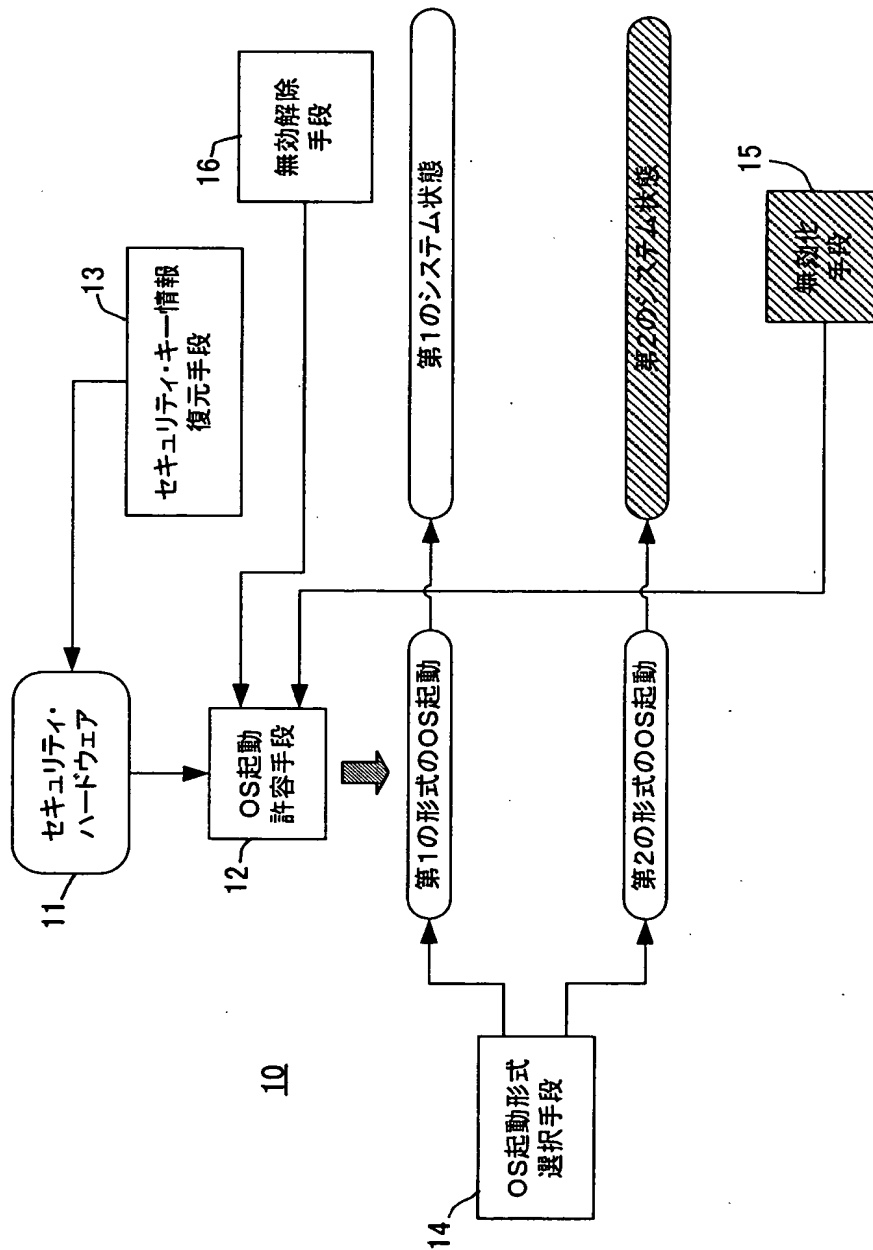
【符号の説明】

10：情報処理装置、11：セキュリティ・ハードウェア、12：OS 起動許容手段、13：セキュリティ・キー情報復元手段、14：OS 起動形式選択手段、15：無効化手段、16：無効解除手段、21：補助記憶装置、22：OS、23：第1の形式のOS 起動の実施手段、24：第2の形式のOS 起動の実施手段、25：所定ユーザ操作の検出手段、26：切替手段、34：メディア検出手段、。

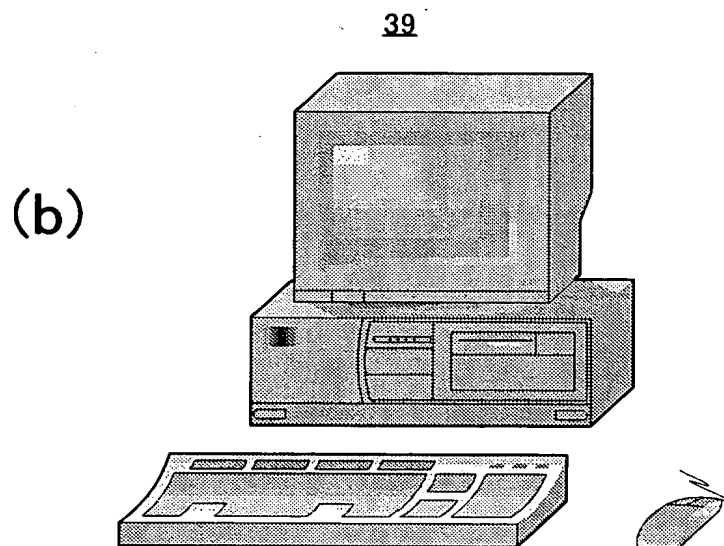
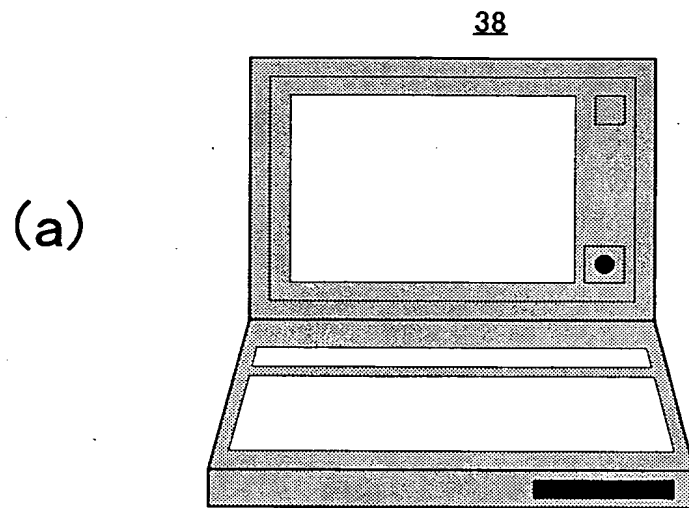
【書類名】

図面

【図 1】



【図 2】



【図 3】

セキュリティ・ハードウェアに基づく
ユーザ認証用窓

ユーザ名:

パスフレーズ:

【図 4】

OSに基づくユーザ認証用窓

ユーザ名:

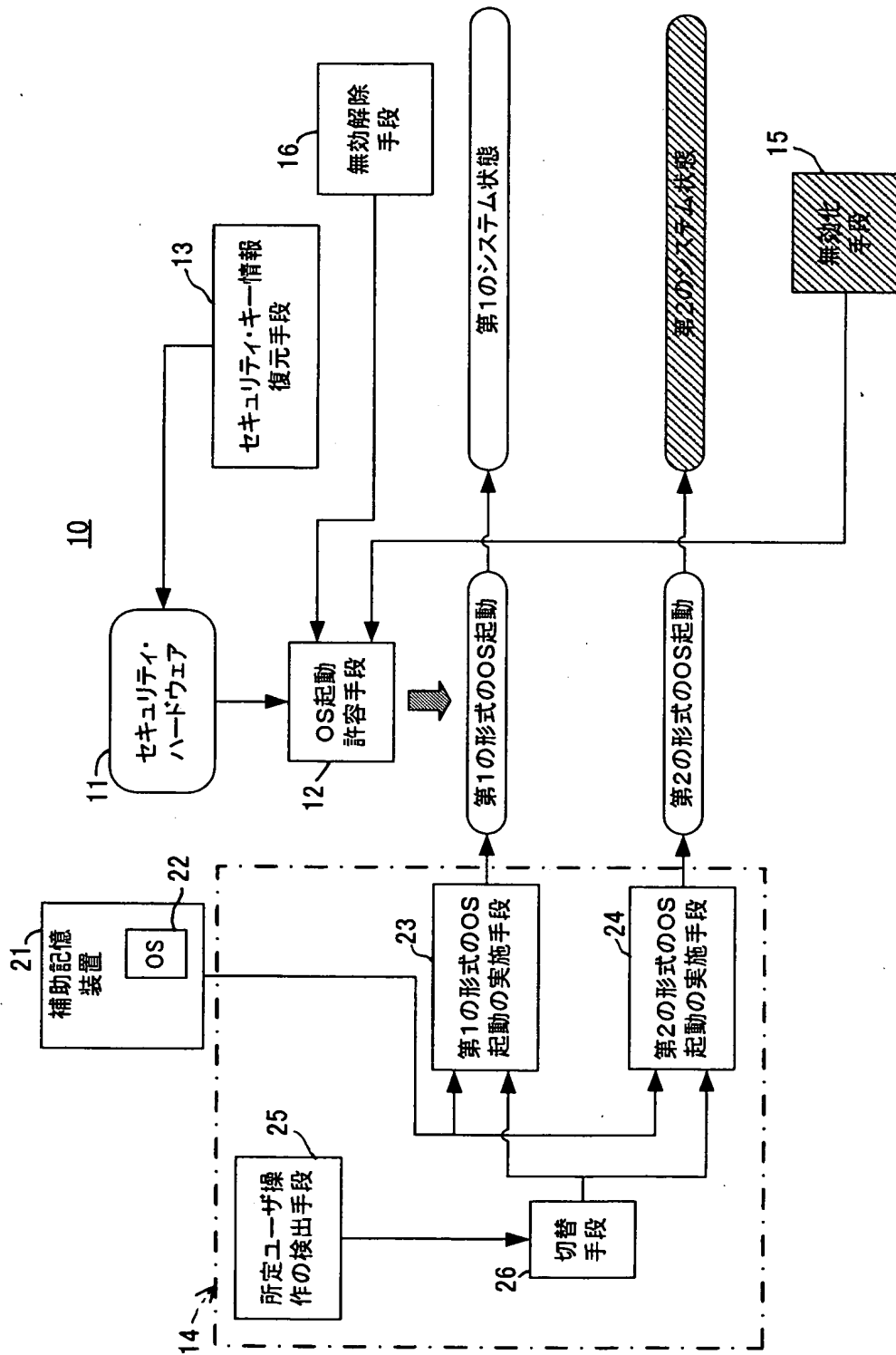
パスワード:

【図 5】

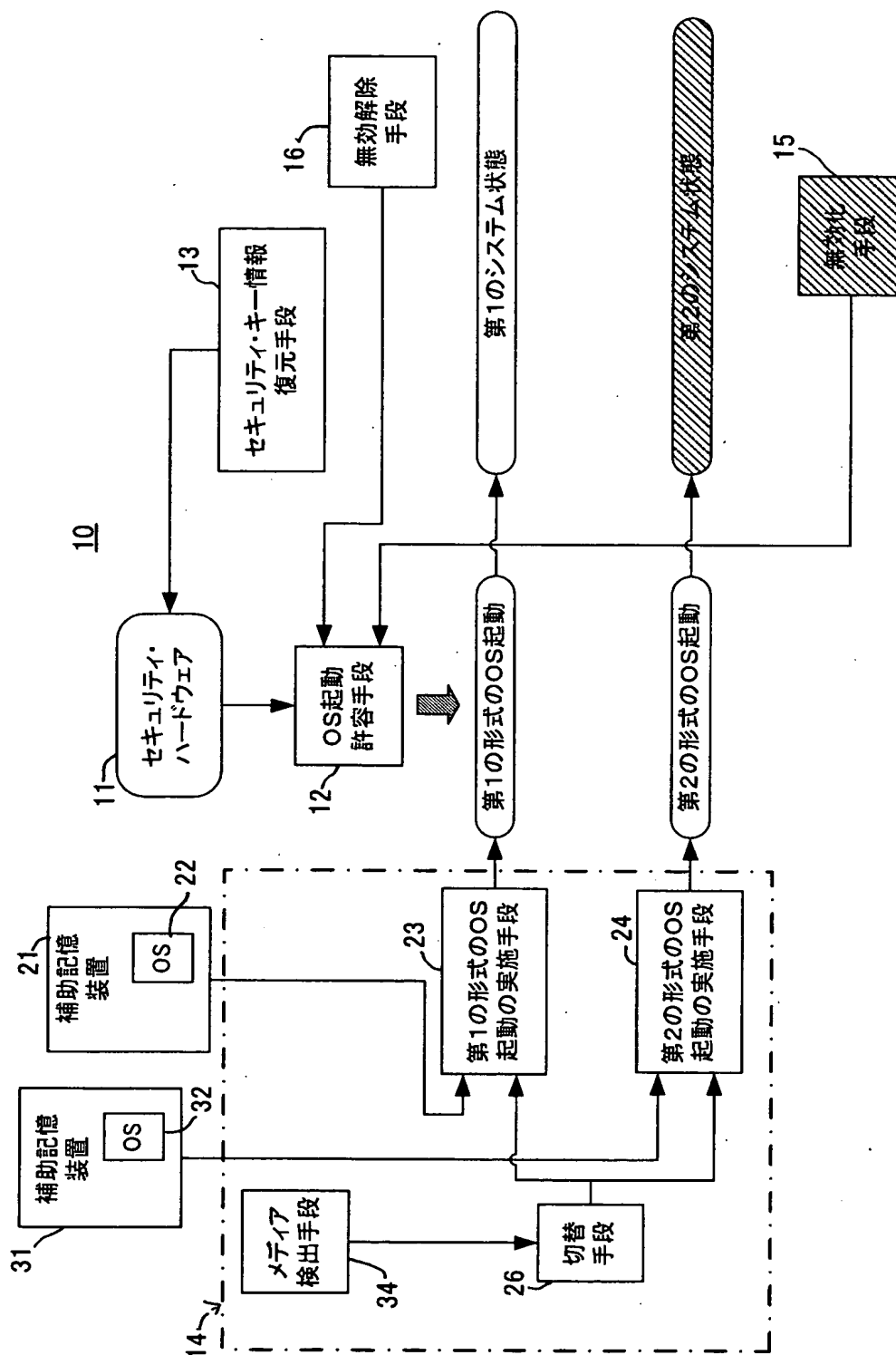
セキュリティ・キー復元用窓

アーカイブ・ファイル の入力	<input type="text" value="A:%recovery.arc"/>	<input type="button" value="参照"/>
公開鍵ファイル の入力	<input type="text" value="C:%key%recovery_pub.key"/>	<input type="button" value="参照"/>
秘密鍵ファイル の入力	<input type="text" value="C:%key%recovery_sec.key"/>	<input type="button" value="参照"/>
<input type="button" value="OK"/> <input type="button" value="キャンセル"/>		

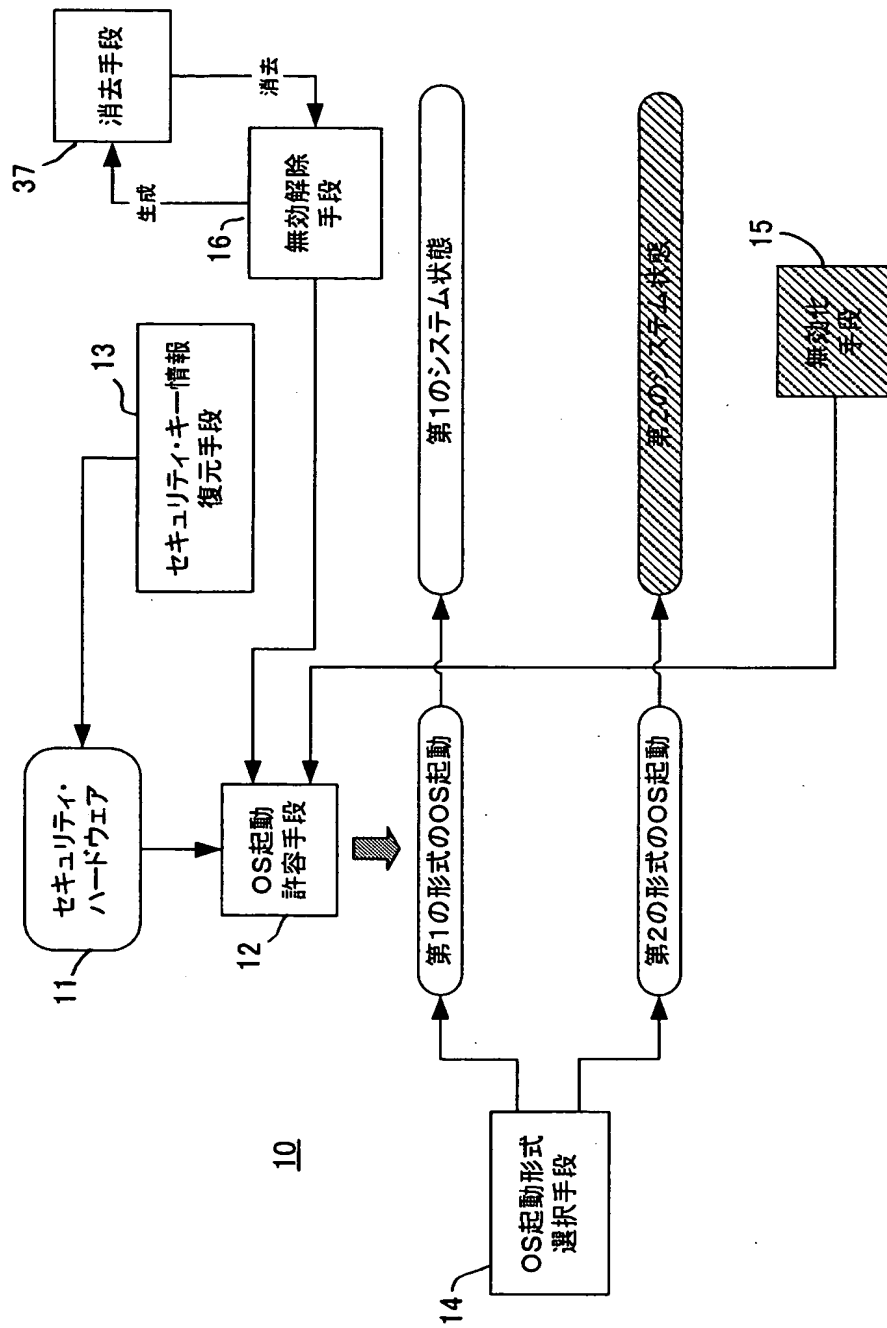
【図6】



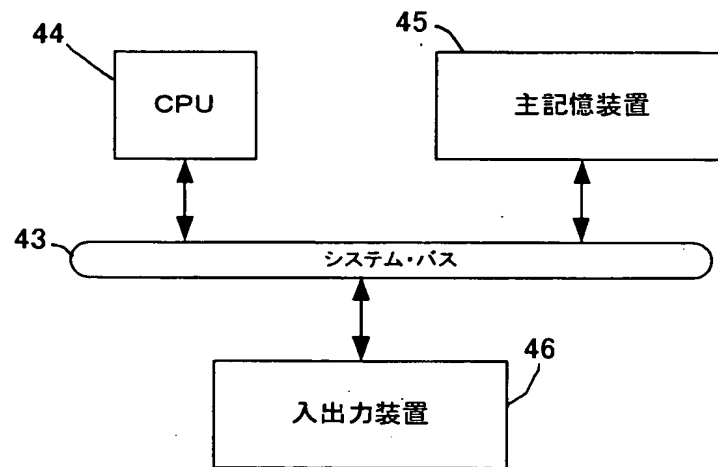
【図 7】



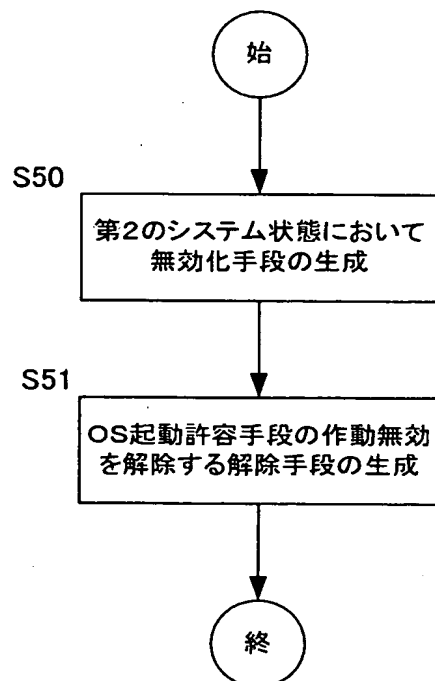
【図 8】



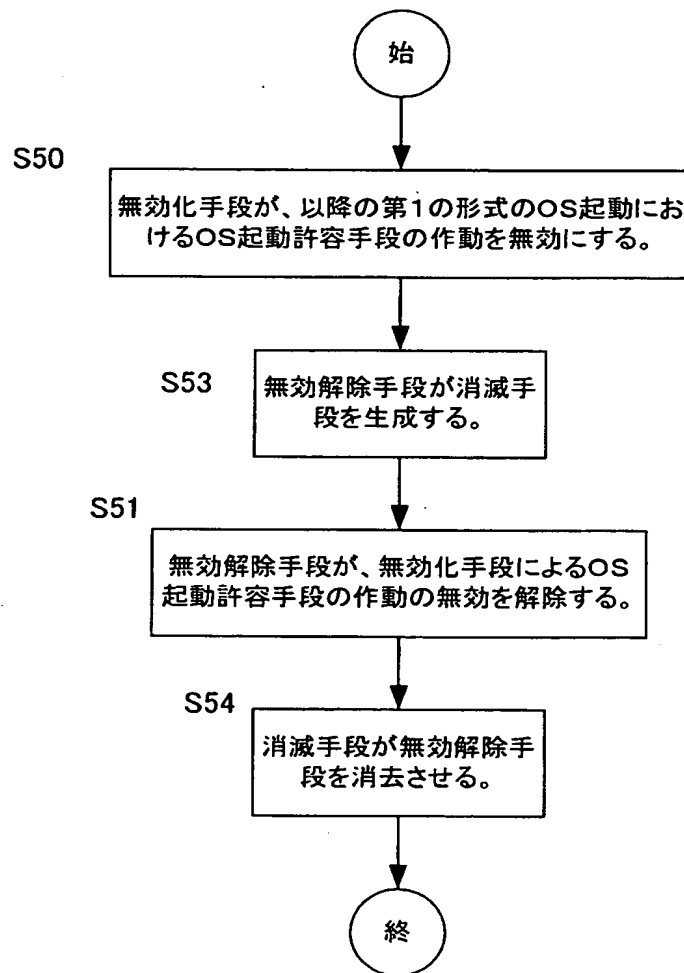
【図 9】



【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 OS 起動時にセキュリティ・ハードウェア 11 のセキュリティ・キー情報に基づいてユーザ認証を行う情報処理装置 10 において、故障修理により交換した後のセキュリティ・ハードウェア 11 に交換前のセキュリティ・キー情報を復元する。

【解決手段】 無効化手段 15 は、セーフ・モード等の機能制限された第 2 の形式の OS 起動により生じる第 2 のシステム状態において、生成される。第 1 の形式の OS 起動では、通常は、セキュリティ・ハードウェア 11 のセキュリティ・キー情報に基づくユーザ認証が実施されるが、無効化手段 15 はこれを無効化する。これにより、ユーザ認証を受けずに、情報処理装置 10 を第 1 のシステム状態にでき、セキュリティ・キー情報の復元が可能になる。無効解除手段 16 はユーザ認証の無効化を解除し、セキュリティ・キー情報の復元後では、第 1 の形式の OS 起動時のユーザ認証が復活する。

【選択図】 図 1

認定・付加情報

特許出願の番号 特願 2003-029813
受付番号 50300192970
書類名 特許願
担当官 塩野 実 2151
作成日 平成15年 2月 7日

<認定情報・付加情報>

【提出日】 平成15年 2月 6日
【特許出願人】
【識別番号】 390009531
【住所又は居所】 アメリカ合衆国 10504、ニューヨーク州 アーモンク ニュー オーチャード ロード
【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション
【代理人】
【識別番号】 100086243
【住所又は居所】 神奈川県大和市下鶴間 1623 番地 14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】 坂口 博
【代理人】
【識別番号】 100091568
【住所又は居所】 神奈川県大和市下鶴間 1623 番地 14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】 市位 嘉宏
【代理人】
【識別番号】 100108501
【住所又は居所】 神奈川県大和市下鶴間 1623 番 14 日本アイ・ビー・エム株式会社 知的所有権
【氏名又は名称】 上野 剛史
【復代理人】 申請人
【識別番号】 100085408
【住所又は居所】 東京都中央区日本橋 2 丁目 1 番 1 号 櫻正宗ビル 9 階
【氏名又は名称】 山崎 隆

次頁無

特願 2003-029813

出 願 人 履 歴 情 報

識別番号

[390009531]

1. 変更年月日

2000年 5月16日

[変更理由]

名称変更

住 所

アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名

インターナショナル・ビジネス・マシーンズ・コーポレーション

2. 変更年月日

2002年 6月 3日

[変更理由]

住所変更

住 所

アメリカ合衆国10504、ニューヨーク州 アーモンク ニュー オーチャード ロード

氏 名

インターナショナル・ビジネス・マシーンズ・コーポレーション